Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Aufgaben zur Klausurvorbereitung (10 ECTS)

Anmerkungen:

(1) Als Hilfsmittel ist nur ein Taschenrechner erlaubt.

(2) Zur Lösung einer Aufgabe gehören auch Darstellung des Lösungswegs und Begründungen.

(3) Großbuchstaben werden in der Klausur in folgender Weise mit Zahlen identifiziert:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

(4) Folgende Tabelle kann beispielsweise bei der VIGENERE-Verschlüsselung verwendet werden. Sie beschreibt die „Addition“ $(x, y) \mapsto x + y \bmod 26$ für Buchstaben. Bei Bedarf wird die Tabelle auch in der Klausur zur Verfügung gestellt.

$f(x,y)$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Aufgabe 1: Das Schlüsselwort „ERLANGEN“ liefert eine MASC-Verschlüsselungsabbildung f.

(1) Beschreibe f durch eine Tabelle.
(2) Gib ein längeres und ein kürzeres Schlüsselwort an, das die gleiche Abbildung f liefert.
(3) Ein Wort wurde mit dem angegebenen Schlüsselwort zu `BJQXNVWSQQN` MASC-verschlüsselt. Bestimme es.

Aufgabe 2: Die ALBC-2-Verschlüsselung mit dem Schlüssel $(1, 0, 4, 0, 1, 7)$ kann auch als VIGENERE-Verschlüsselung gedeutet werden. Welches VIGENERE-Schlüsselwort beschreibt diese Verschlüsselung?

Aufgabe 3: Der folgenden PLAYFAIR-Verschlüsselung liege das Schlüsselwort „ERLANGEN“ zugrunde.

(1) Stelle die zugehörige PLAYFAIR-Matrix auf.
(2) Erläutere die PLAYFAIR-Verschlüsselung an Hand der Verschlüsselung von „HENKELTASSE“.
(3) Entschlüssle den Chiffretext „RQ AU RL UK LZ ER“, der mit obigem Schlüsselwort PLAYFAIR-verschlüsselt wurde.

Aufgabe 4: Peter schickt an Michael folgende VIGENERE-verschlüsselte Nachricht:

```
HMPUAV XBYLLXH, MNA SMWE IMC XERPG JIFXJ JPKJWPAWTATNEE DWYQXJ. OLGJWE
WQ QTK RMPEHITVDX PBJ TLTN VLMOGSEWIRX CIMXJ, AZKWYQ BYL LVDXPG
OSWEPI? GBAPP ZNYPLOI AXPIC
```

(1) Bestimme das zugehörige VIGENERE-Schlüsselwort.
(2) Entschlüssle das achte Wort (`JPKJWPAWTATNEE`) der Nachricht.

Aufgabe 5: Der folgende Chiffretext `EDWSQEZXAUNNWXVVZB` ist STROM-verschlüsselt, wobei als Schlüsselstrom die Folge der Primzahlen benutzt wurde. Entschlüssle den Text.

Aufgabe 6: Ein Text wurde mit dem Schlüsselwort `ERLANGEN` TRANSSPA-verschlüsselt zu

`SEGNVESHLNIHURRSLECLOUGTESAM`

Entschlüssle den Text.

Aufgabe 7: Entschlüssle folgenden ADFGVX-chiffrierten Text, wobei beim Verschlüsseln als erstes Schlüsselwort „JANUAR2025“ und als zweites Schlüsselwort „WINTER“ verwendet wurde:

`AGFGD GFXDX FGVVX DFDDA AAXVG GVXFA GXXDD DADGA AAVF`

Erläutere dabei die ADFGVX-Verschlüsselung.

Aufgabe 8: Die Zahlen $m = 6015093799$ und $n = 10872069857$ haben die Primfaktorzerlegungen

$$m = 11^5 \cdot 13^3 \cdot 17 \quad \text{und} \quad n = 11^6 \cdot 17 \cdot 19^2.$$

Bestimme die Primfaktorzerlegungen von

$$\mathrm{ggT}(m,n), \quad \mathrm{kgV}(m,n) \quad \text{und} \quad m+n.$$

Aufgabe 9: Seien $a, b \in \mathbb{Z}$. Zeige: Genau dann ist $10a+b$ durch 19 teilbar, wenn $a+2b$ durch 19 teilbar ist.

Aufgabe 10: Wende den erweiterten euklidischen Algorithmus auf 245 und 126 an und bestimme damit $\mathrm{ggT}(245,126)$ und $x, y \in \mathbb{Z}$ mit $245x + 126y = \mathrm{ggT}(245,126)$.

Aufgabe 11: $(f_n)_{n\geq 0}$ sei die Folge der Fibonacci-Zahlen.

(1) Berechne $f_0, f_1, \ldots, f_{12}$.
(2) Bestimme für jedes $n \geq 1$ eine Lösung der Gleichung

$$f_n x \equiv f_{n+1} \bmod f_{n+2}.$$

(3) Ist die Gleichung

$$f_n x \equiv f_{n+1} \bmod f_{n+3}$$

für jedes $n \geq 1$ lösbar?

Aufgabe 12: Zeige, dass für eine ungerade natürliche Zahl $n > 1$ die Zahl $\frac{n+1}{2}$ invers zu 2 modulo n ist.

Aufgabe 13: Bestimme ein Inverses von a modulo n, das zwischen 0 und $n-1$ liegt, falls ein solches existiert.

(1) $(a,n) = (10, 403)$,
(2) $(a,n) = (109, 4033)$.

Aufgabe 14: Gibt es $a, b \in \mathbb{Z}$, sodass die Gleichung

$$ax \equiv b \bmod 30$$

(1) keine Lösung,
(2) genau eine Lösung modulo 30,
(3) genau 2 Lösungen modulo 30,
(4) genau 4 Lösungen modulo 30,
(5) genau 6 Lösungen modulo 30

besitzt? (Gib Beispiele für a, b an oder begründe die Nichtexistenz.)

Aufgabe 15:

(1) Bestimme die kleinste natürliche Zahl, die das folgende Kongruenzgleichungssystem löst:

$$x \equiv 2 \bmod 25, \quad x \equiv 5 \bmod 52.$$

(2) Warum besitzt das folgende Kongruenzgleichungssystem keine Lösung?

$$x \equiv 4 \bmod 45, \quad x \equiv 5 \bmod 54.$$

Aufgabe 16: Erläutere eine square-and-multiply-Methode an der Berechnung von

$$3^{97} \bmod 100.$$

Aufgabe 17:

(1) Wie kann man $\varphi(n)$ berechnen, wenn man die Primfaktorzerlegung von n kennt?
(2) Berechne $\varphi(100)$.
(3) Was besagt der Satz von Euler über die Eulersche φ-Funktion?
(4) Bestimme die Ordnung von 3 modulo 100.
(5) Was sind die letzten beiden Dezimalstellen von 3^{123}?
(6) Was ist $7^{5001} \bmod 11$?

Aufgabe 18:

(1) Gib zwei Varianten des kleinen Satzes von Fermat an.
(2) Zeige: Ist p eine von 2 und 5 verschiedene Primzahl und n eine natürliche Zahl mit $p-1 \mid n$, so gilt $10^n \equiv 1 \bmod p$.
(3) Gib mindestens 6 verschiedene Primteiler der 60-stelligen Zahl

$$\underbrace{999\ldots999}_{60\text{ Einsen}} = 10^{60} - 1.$$

Aufgabe 19: Ist 645 eine Fermat-Pseudoprimzahl zur Basis 2? (Es ist $645 = 3 \cdot 5 \cdot 43$.)

Aufgabe 20:

(1) Was ist eine Carmichael-Zahl?
(2) Was besagt das Korselt-Kriterium?
(3) Zeige, dass 561 eine Carmichael-Zahl ist.
(4) Warum kann eine RSA-Zahl $N = pq$ keine Carmichael-Zahl sein? (Hinweis: $pq - 1 = p(q-1) + (p-1)$)

Aufgabe 21:

(1) Beschreibe den Miller-Rabin-Test (zur Basis 2). Welche Ergebnisse sind möglich?
(2) Teste $n = 21$ mit dem Miller-Rabin-Test (zur Basis 2).
(3) Zeige: Ist n eine natürliche Zahl mit $n \equiv 1 \bmod 4$ und gilt $4^{\frac{n-1}{4}} \equiv -1 \bmod n$, so besteht n den Miller-Rabin-Test zur Basis 2.

Aufgabe 22: Zeige: Besteht eine ungerade natürliche Zahl n den Miller-Rabin-Test zur Basis 2, so besteht n auch den Fermat-Test zur Basis 2.

Aufgabe 23:

(1) Ist 25 eine Fermat-Pseudoprimzahl zur Basis 7?
(2) Ist 25 eine Miller-Rabin-Pseudoprimzahl zur Basis 7?

Aufgabe 24: Zeige: Jede zusammengesetzte ungerade natürliche Zahl n ist eine Miller-Rabin-Pseudoprimzahl zur Basis $a = n - 1$.

Aufgabe 25: $(N, e) = (55, 27)$ ist ein öffentlicher RSA-Schlüssel.

(1) Bestimme einen zu $(55, 27)$ passenden privaten RSA-Schlüssel $(55, d)$.
(2) Ein aus vier Großbuchstaben bestehendes Wort wurde nach dem Schema der Vorbemerkungen in eine Zahlenfolge a_1, a_2, a_3, a_4 umgewandelt, dann mit dem Schlüssel $(55, 27)$ zur Zahlenfolge 33,9,8,24 RSA-verschlüsselt. Entschlüssle es.

Aufgabe 26: Sei (N, e) ein öffentlicher RSA-Schlüssel mit $N \equiv 2 \bmod 3$. Zeige, dass dann $e \geq 5$ gilt.

Aufgabe 27: $N = 89425157$ ist eine RSA-Zahl.

(1) Faktorisiere N mit der Fermatschen Faktorisierungsmethode.
(2) Bestimme die kleinste natürliche Zahl $e > 1$, sodass (N, e) ein gültiger (öffentlicher) RSA-Schlüssel ist.

Aufgabe 28: Von der RSA-Zahl $N = 848731787$ kennt man $\varphi(N) = 848673456$. Faktorisiere N.

Aufgabe 29: $N = 2699773523$ ist eine RSA-Zahl. Für $w = 20427359$ gilt $w^2 \equiv 1 \bmod N$.

(1) Bestimme alle $x \in \{0, 1, \ldots, N-1\}$ mit $x^2 \equiv 1 \bmod N$.
(2) Faktorisiere N.

Aufgabe 30: Für $N \in \mathbb{N}$ sei $Q_N = \{a \in \mathbb{Z} : 0 \leq a \leq N-1, a^2 \equiv 1 \bmod N\}$ die Menge der Quadratwurzeln von 1 modulo N. $N = 11592649$ hat die Primfaktorzerlegung $N = pq$ mit $p = 2713$ und $q = 4273$. Bestimme Q_N.

Aufgabe 31: Bestimme die Kettenbruchentwicklung von $\frac{1234}{4321}$ und die zugehörigen Näherungsbrüche.

Aufgabe 32: $(N, e) = (57174151, 3291863)$ ist ein öffentlicher RSA-Schlüssel. Der private Exponent d kommt im 5. Näherungsbruch von $\frac{e}{N}$ vor.

(1) Bestimme den 0., 1., 2., 3., 4., und 5. Näherungsbruch von $\frac{e}{N}$.
(2) Bestimme den privaten Exponenten d.
(3) Bestimme $\varphi(N)$.

Aufgabe 33: Eine Folge $(x_i)_{i\geq 0}$ hat die Vorperiode $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$ und die Periode $31, 37, 41, 43$. Bestimme den kleinsten Index $\ell \in \mathbb{N}$ mit $x_\ell = x_{2\ell}$.

Aufgabe 34: Zeige: Ist p ein Primteiler einer Fermat-Zahl $F_n = 2^{2^n} + 1$ (mit $n \in \mathbb{N}_0$), so hat 2 Ordnung 2^{n+1} modulo p.

Aufgabe 35: Bestimme alle Primzahlen p, für die $\operatorname{ord}_p(4) = 11$ gilt.

Aufgabe 36: Sei p eine Primzahl, sodass auch $\frac{p-1}{2}$ eine Primzahl ist.

(1) Zeige: Gilt $2^{\frac{p-1}{2}} \not\equiv 1 \bmod p$, so ist 2 eine Primitivwurzel modulo p.
(2) Was ist $2^{\frac{p-1}{2}} \bmod p$, wenn $2^{\frac{p-1}{2}} \not\equiv 1 \bmod p$ gilt?

Aufgabe 37:

(1) Bestimme die Ordnung von 4 modulo 13.
(2) Bestimme alle natürlichen Zahlen n, für die $\frac{4^n+1}{13}$ eine natürliche Zahl ist. (Hinweis: Dies lässt sich durch eine Kongruenzbedingung charakterisieren.)

Aufgabe 38: Sei $p \geq 5$ eine Primzahl und 2 eine Primitivwurzel modulo p. Zeige: Genau dann ist 8 eine Primitivwurzel modulo p, wenn $p \equiv 2 \bmod 3$ gilt.

Aufgabe 39: Für ihren Diffie-Hellman-Schlüsselaustausch verwenden Andrea und Birgit die Parameter $(p, g) = (101, 2)$. Die öffentlichen Schlüssel von Andrea und Birgit sind $f_A = 27$ und $f_B = 72$.

(1) Zeige, dass $g = 2$ eine Primitivwurzel modulo $p = 101$ ist.
(2) Berechne den privaten Schlüssel von Andrea oder Birgit.
(3) Bestimme den gemeinsamen Diffie-Hellman-Schlüssel von Andrea und Birgit.

Aufgabe 40: $(p, g, f) = (29, 2, 4)$ ist ein öffentlicher ElGamal-Schlüssel.

(1) Bestimme den zugehörigen privaten ElGamal-Schlüssel (p, g, e).
(2) Ein aus vier Großbuchstaben bestehendes Wort wurde nach dem Schema der Vorbemerkungen in eine Zahlenfolge a_1, a_2, a_3, a_4 umgewandelt und dann mit dem Schlüssel (p, g, f) zur Folge

(b_i, c_i) chiffriert:

$$(18, 7), \quad (14, 18), \quad (21, 27), \quad (26, 7).$$

Entschlüssle den Text.

Aufgabe 41: Zu einem öffentlichen RSA-Schlüssel $(N, e) = (5893, 3)$ werden Dokumente mit Hashwerten h_i und zugehörigen RSA-Signaturen s_i gefunden. Welche der Signaturen sind gültig, welche ungültig?

$$(h_1, s_1) = (1111, 2925), \quad (h_2, s_2) = (2222, 2018), \quad (h_3, s_3) = (3333, 3208).$$

Aufgabe 42: Für nachfolgende ElGamal-Signatur wird der private Schlüssel $(p, g, e) = (1283, 5, 17)$ benutzt.

(1) Bestimme den zugehörigen öffentlichen Schlüssel (p, g, f).
(2) Signiere ein Dokument mit Hashwert $h = 123$ unter Verwendung der kleinstmöglichen „Zufallszahl“ z, die größer als 1 ist.

Aufgabe 43: Andreas öffentlicher ElGamal-Signatur-Schlüssel ist $(p, g, f) = (5557, 5, 1313)$. Es ist bekannt, dass Andrea zum Signieren als „Zufallszahl“ z gerne die Zahl 3305 nimmt. Ein Dokument mit Hashwert $h = 3042$ und Andreas Signatur $(b, c) = (7, 10)$ wird gefunden. Bestimme Andreas privaten Schlüssel.

Aufgabe 44: Ute verwendet die ElGamal-Signatur mit dem öffentlichen Schlüssel $(p, g, f) = (15083, 5, 1773)$. Vera schaut sich Signaturen von Ute an und stößt dabei auf die zwei Signaturen $(15081, 10179)$, $(15081, 10178)$ zu den Hashwerten 12668 und 7719. Was fällt Vera auf? Was ist der private Schlüssel von Ute?

Aufgabe 45: Um den diskreten Logarithmus von a zur Basis g modulo p zu mit der Pollard-ρ-Methode zu berechnen, zerlegt man $\{1, \ldots, p-1\}$ in drei disjunkte Mengen S_1, S_2, S_3 und definiert dann Folgen x_i, e_i, f_i rekursiv wie folgt: $(x_0, e_0, f_0) = (1, 0, 0)$ und

$$(x_{i+1}, e_{i+1}, f_{i+1}) = \begin{cases} (ax_i \bmod p, (e_i + 1) \bmod (p-1), f_i), & \text{falls } x_i \in S_1, \\ (x_i^2 \bmod p, (2e_i) \bmod (p-1), (2f_i) \bmod (p-1)), & \text{falls } x_i \in S_2, \\ (gx_i \bmod p, e_i, (f_i + 1) \bmod (p-1)), & \text{falls } x_i \in S_3. \end{cases}$$

Warum ist die Zerlegung

$$\begin{aligned} S_1 &= \{x \in \{1, \ldots, p-1\} : x \equiv 0 \bmod 3\}, \\ S_2 &= \{x \in \{1, \ldots, p-1\} : x \equiv 1 \bmod 3\}, \\ S_3 &= \{x \in \{1, \ldots, p-1\} : x \equiv 2 \bmod 3\} \end{aligned}$$

schlecht?

Aufgabe 46: Um den diskreten Logarithmus von a zur Basis g modulo p zu mit der Pollard-ρ-Methode zu berechnen (mit einer Primitivwurzel g modulo p), wurde in der Vorlesung eine Folge (x_i, e_i, f_i) (mit

$x_i \in \{1, \ldots, p-1\}$, $e_i, f_i \in \{0, \ldots, p-2\}$ und $x_i \equiv a^{e_i} g^{f_i} \bmod p$) rekursiv durch $(x_0, e_0, f_0) = (1, 0, 0)$ und

$$(x_{i+1}, e_{i+1}, f_{i+1}) = \begin{cases} (ax_i \bmod p, (e_i + 1) \bmod (p-1), f_i), & \text{falls } x_i \equiv 1 \bmod 3, \\ (x_i^2 \bmod p, (2e_i) \bmod (p-1), (2f_i) \bmod (p-1)), & \text{falls } x_i \equiv 2 \bmod 3, \\ (gx_i \bmod p, e_i, (f_i + 1) \bmod (p-1)), & \text{falls } x_i \equiv 0 \bmod 3 \end{cases}$$

definiert.
$g = 2$ ist eine Primitivwurzel modulo $p = 101$. Mit der Pollard-ρ-Methode soll der diskrete Logarithmus von $a = 3$ zur Basis $g = 2$ modulo $p = 101$ bestimmt werden. Hier sind die ersten Glieder der zugehörigen Folge $((x_i, e_i, f_i, x_{2i}, e_{2i}, f_{2i}))_{i \geq 0}$:

$(1, 0, 0, 1, 0, 0), (3, 1, 0, 6, 1, 1), (6, 1, 1, 24, 1, 3), (12, 1, 2, 96, 1, 5), (24, 1, 3, 71, 2, 6), (48, 1, 4, 81, 8, 24),$
$(96, 1, 5, 82, 9, 25), (91, 1, 6, 17, 20, 50), (71, 2, 6, 73, 40, 1), (92, 4, 12, 87, 82, 2), (81, 8, 24, 17, 83, 3),$
$(61, 8, 25, 73, 66, 7), (82, 9, 25, 87, 34, 14), (44, 10, 25, 17, 35, 15), (17, 20, 50, 73, 70, 31),$
$(87, 40, 0, 87, 42, 62), \ldots$

Bestimme damit den diskreten Logarithmus von 3 zur Basis 2 modulo 101.

Aufgabe 47: Sei $p = 31$.

(1) Zeige, dass 3 eine Primitivwurzel modulo p ist.
(2) Bestimme den diskreten Logarithmus von 2 zur Basis 3 modulo p mit der $(p-1)$-Methode.

Aufgabe 48: Für $p = 307$ ist $g = 5$ eine Primitivwurzel. Definiert man $m = \lceil \sqrt{p-1} \rceil$ und B durch $B(g^i \bmod p) = i$ für $0 \leq i \leq m-1$, so erhält man folgende Tabelle:

x	1	5	25	125	11	55	275	147	121	298	262	82	103	208	119	288	212	139
$B(x)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Berechne für $a = 3$

$$h_j = ag^{-mj} \bmod p$$

für $j = 0, 1, 2, \ldots$ soweit nötig, um damit und der oben stehenden Tabelle den diskreten Logarithmus von 3 zur Basis 5 modulo 307 (mit der baby-step-giant-step-Methode) zu bestimmen.